$$\sum\left(y-\bar{y}\right)^2 = 3^2 + \left(-4\right)^2 + 1^2 \approx 9 + 16 + 1 = 26$$

$$\sqrt{34.67 \times 26} = \sqrt{901.4} \approx 30.02$$

Производим финальный расчет подставив числитель и знаменатель: $r_{xy} \approx 0.999$. Значение почти равно 1. Это значит, что зависимость практически идеальна.

Затем необходимо описать закон сокращения длительности визуальных эпох. Анализ временных рядов показал, что и в искусстве, и в интерфейсах процесс подчиняется закону экспоненциального убывания. Для аппроксимирования использовалась такая функция:

$$T\left(n\right) = T_0 \times e^{-\lambda n},$$

где $T(n)$ – длительность n-го цикла, T_0 – начальная длительность, λ – показатель экспоненты сжатия.

В эпохах художественных стилей практически все время встречается одна и та же закономерность – каждый новый срок короче предыдущего вдвое. Поэтому $\lambda_{art} = 0.69$.

В смене интерфейсов нет устоявшейся закономерности:

$$\frac{13}{20} \approx 0.65, \quad \frac{7}{13} \approx 0.54,$$

$$e^{-\lambda} = 0.595, \quad \lambda_{UI} = 0.52$$

Искусство «сжималось» быстрее, а интерфейсы «сжимаются» плавнее, но оба процесса – это экспоненциальный распад времени.

Заключение

Исследование выявило и математически обосновало цикличность развития графических интерфейсов. Сопоставление эволюции художественных стилей XV-XXI веков с историей цифровых интерфейсов подтвердило: дизайн подчиняется универсальным законам смены парадигм, но в ускоренном темпе.

Современные интерфейсы не возвращаются к скевоморфизму, а переходят на новый уровень – «статическая сложность» сменяется «динамической» благодаря снятию аппаратных ограничений. Анализ показал близость стадий трансформации у ключевых компаний.

Текущее усложнение интерфейсов закономерно и прогнозируемо, а дальнейшее развитие UI-дизайна связано с интеграцией AR и стиранием границ между интерфейсом и реальностью.

Список литературы

1. Гомбрих Э. История искусства. М.: Искусство – XXI век, 2013.

2. Иконки приложений [Электронный ресурс]. URL: https://logos.fandom.com (дата обращения: 08.12.2025).

3. Иконки приложений [Электронный ресурс]. URL: https://wikipedia.org (дата обращения: 08.12.2025).

4. Уолтер А. Эмоциональный веб-дизайн. М.: Манн, Иванов и Фербер, 2012.

5. K. Lee Towards a Working Definition of Designing Generative User Interfaces // DIS '25 Companion, July 5–9. 2025. Funchal, Portugal.

ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ И ИНВЕСТИЦИИ В КИБЕРБЕЗОПАСНОСТИ

Ярошенко Е. А., Мозговенко А. А.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь, e-mail: ya@amozgovenko.ru

Задачи исследования:

1. Классифицировать существующие методы оценки экономической эффективности ИБ-инвестиций по критериям:

– тип измеряемых выгод (материальные/нематериальные);

– горизонт планирования;

– требуемые входные данные.

2. Сопоставить методы с этапами процесса управления рисками (идентификация, анализ, реагирование, мониторинг).

Материалы и методы исследования

Современные исследования в области экономики кибербезопасности фокусируются на:

– Квантификации рисков. Работы 2023–2025 гг. развивают модели вероятностной оценки ущерба (FAIR, Cyber Value at Risk), включая каскадные эффекты и репутационные потери. Активно внедряются ML методы для прогнозирования частоты инцидентов.

– ROI метрики для ИБ. Публикуются адаптации классических финансовых показателей (NPV, IRR) под специфику ИБ проектов, где выгоды носят отсроченный и неденежный характер. Обсуждается проблема «тёмной материи» ИБ инвестиций (неучтённые косвенные эффекты).

– Регуляторное влияние. Исследования оценивают затраты на соответствие GDPR, NIS2, ФЗ 152 и др., а также экономический эффект от штрафов за нарушения.

Основная цель – создать методологическую базу для обоснованного распределения инвестиций в кибербезопасность на основе риск-ориентированного подхода.

Результаты исследования и их обсуждение

По данным исследования Gartner кибербезопасность и информационная безопасность занимает первое место в списке запланированных инвестиций на 2022 год, 66% респондентов ожидают увеличения инвестиций в эту сферу [1].

Исследования Accenture свидетельствуют о том, что бюджеты безопасности увеличиваются, более 82% респондентов сказали, что бюджет увеличился в течение 2021 года.

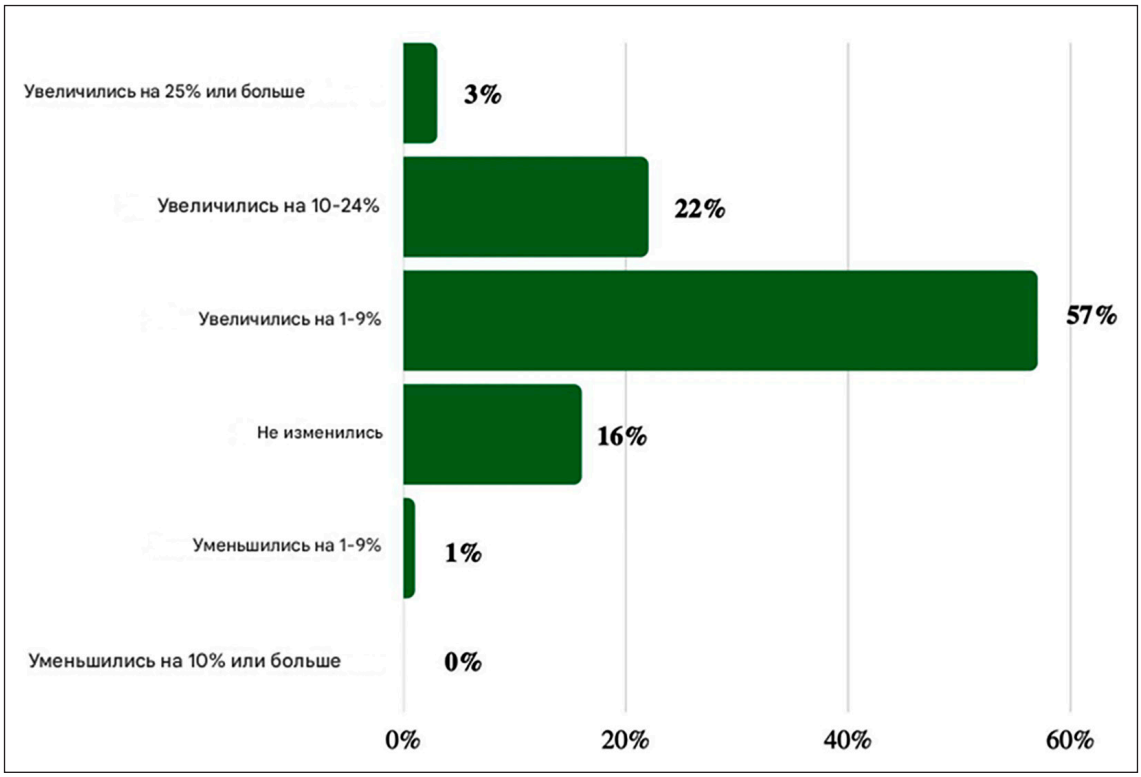

Рис. 1. Увеличение расходов на кибербезопасность в 2021 году по сравнению с 2020 г.

Рис. 2. Увеличение среднего количества атак в 2021 году по сравнению с 2020 г.

Бюджеты на безопасность составляют до 15% от общих расходов на ИТ, что на 5% пунктов больше, чем расходы в 2020 году. На рисунке 1 изображены данные по увеличению расходов на кибербезопасность в 2021 году по сравнению с 2020 годом [2].

По данным Accenture в течение 2021 года на одну компании было в среднем 270 атак, что на 31% больше, чем в 2020 году. На рисунке 1.2 изображены данные по увеличению атак в 2021 году по сравнению с 2020 годом [2].

Из-за того, что последствия от определенных атак приводят к значительным репутационным и финансовый ущерб, организация должна инвестировать в кибербезопасность, что позволит избежать определенных киберугроз или потенциально минимизировать последствия успешной реализации киберугроз.

Из-за определенных технических и экономических факторов организации не могут обеспечить совершенный уровень безопасности. Организации обычно планируют ежегодный ограниченный бюджет по кибербезопасности, поэтому перед уполномоченными лицами стоит трудная задача по эффективному распределению данного бюджета. Возникает задача по принятию решения о распределении бюджета по кибербезопасности.

В общем виде процесс принятия решений можно разделить на следующие этапы:

– Характеристика проблемы
– Определение альтернатив
– Определение критериев
– Выбор метода принятия решения
– Оценка альтернатив по критериям
– Проверка решения на соответствие поставленной проблеме [3].

Более подробно рассмотрим каждый из этапов.

Характеристика проблемы

Цель данного этапа – это четкое определение проблемы и описание целей. Лица, принимающие решения, должны согласовать этот вопрос между собой, и кратко и четко описать проблему: определить текущее состояние, цели и требования к решению.

Определение альтернатив

Цель данного этапа – это определение альтернативных решений поставленной проблемы. Каждое решение должно удовлетворять требованиям.

Определение критериев

Цель данного этапа – это выбор критериев, по которым будут оцениваться альтернативные решения. Если количество критериев довольно значительно, то есть смысл объединить их в группы [3].

Выбор метода принятия решения

Существует много способов принятия решения. Выбор метода зависит от поставленной проблемы, количества альтернативных решений и критериев. Также существуют методы, являющие собой сочетание определенных методов.

Оценка альтернатив по критериям

Цель данного этапа – это оценка альтернативных решений по определенным критериям, с помощью выбранного метода.

Проверка решения на соответствие поставленной проблеме

Принятое решение обязательно следует проверять на соответствие поставленным целям и требованиям. Если решение не соответствует, следует пересмотреть альтернативные решения и критерии оценки данных решений.

Существует много методов и подходов, которые используются для оценки инвестиций и принятия решений о распределении бюджета. D. Schatz и R. Bashroush сделали обзор ключевых подходов подробно рассмотрев 25 различных работ по данной тематике, были описаны используемые подходы, их ключевые элементы, преимущества и недостатки.[4]

Также на основе рассмотренных работ были выделены следующие категории методов и подходов к оценке инвестиций:

– AHP (The Analytic Hierarchy Process) – метод анализа иерархий (МАИ), это метод, при котором происходит декомпозиция проблемы: определение цели, критериев оценки и альтернатив, и проводится оценка альтернатив по определенным критериям с помощью попарных сравнений.

– DSS (Decision Support Systems) – системы поддержки принятия решений, это структурированный процесс, помогающий принимать решения более эффективно.

– Game Theory – теория игр, помогающая смоделировать ситуацию (например противодействия «злоумышленник-защитник») и предусмотреть последствия для оптимального принятия решения в условиях конкуренции или конфликта.

– NPV (Net Present Value) – чистая текущая стоимость, используемая для предсказания доходности инвестиции, в общем виде она определяется, как разница стоимости ожидаемых денежных потоков, на сегодня и стоимости инвестиций, на сегодня.

– ROA (Return on Attack) – рентабельность атаки – это расширение ROI, где рассчитывается рентабельность инвестиций злоумышленника, его выгода и расходы.

– ROI (Return on Investment) – рентабельность инвестиций, рассчитывается рентабельность инвестиций, помогающая оценить на сколько выгоден тот или иной денежный вклад.

– ROI, NPV – комбинация рентабельности инвестиций и чистой текущей стоимости.

– ROT (Real Options Theory) – теория реальных опционов, помогающая количественно оценить уровень гибкости, свойственной процессу принятия решений.

– UM (Utility maximization) – максимизация полезности, концепция в которой субъект пытается извлечь наибольшую выгоду из инвестиций [4].

Более подробно рассмотрим некоторые из исследований и работ.

В частности, в работе «Evaluating Information Security Investments Using the ANALYTIC HIERARCHY PROCESS» используется МАИ для оценки инвестиций в информационную безопасность. Они отмечают, что МАИ является полезным инструментом, помогающим организации в принятии инвестиционных решений. Но при использовании данного метода важно и лицо, принимающее решение, поскольку именно он определяет критерии, подкритерии и оценивает [5].

В работе «Measuring the Risk-Based Value of IT Security Solutions» рассматривается подход RROI (Risk-based return on investment) для определения затрат и преимуществ решений по информационной безопасности. Данный метод подходит для определения суммы инвестиций и определяет, что важным критерием при оценке ИТ-решений является польза от инвестиции посредством уменьшения ожидаемых потерь или риска [6].

В работе «An economic modelling approach to information security risk management» представлен подход, позволяющий осуществлять экономическое моделирование процесса управления рисками информационной безопасности. В данном подходе используются оценка рисков, расчет ROSI (Return on Security Investment), NPV и IRR (Internal Rate of Return) [7].

Большое количество работ по теме оценки инвестиций в информационную и кибербезопасность свидетельствует об актуальности дан-

ной проблемы. Среди рассматриваемых работ многие модели для оценки инвестиций базировались на оценке рисков киберугроз. Оценка рисков помогает понять текущие киберугрозы и эффективно распределить инвестиции на улучшение кибербезопасности и минимизацию рисков киберугроз в ИС.

Выводы

Обоснованная оценка инвестиций в кибербезопасность возможна только при тесной связке финансовых метрик с процессами управления рисками. Предложенные методы и рекомендации позволяют:

– повышать прозрачность бюджетирования ИБ;

– аргументировать приоритеты защиты перед руководством;

– адаптировать стратегии под эволюцию угроз.

Дальнейшая работа должна фокусироваться на автоматизации расчётов и создании открытых баз данных по стоимости инцидентов.

Список литературы

1. Gartner Survey of Over 2,000 CIOs Reveals the Need for Enterprises to Embrace Business Composability in 2022, STAMFORD, Conn. Октябрь 18, 2021.

2. Fülöp J. Introduction to decision making methods // BDEI-3 workshop, Washington, 2005. С. 1-15.

3. Schatz D., Bashroush R. Economical valuation for information security investment: systematic literature review // Inf Syst Front 19, 2017. С. 1205-1228.

4. Bodin L. D., Gordon L. A., Loeb M. P. Evaluating information security investments using the analytic hierarchy process // Communications of the ACM. 2005. № 48(2). С. 79-83.

5. Arora A., Hall D., Piato C. A., Ramsey D., Telang R. Measuring the risk-based value of IT security solutions, 2004. P. 35-42.

6. Bojanc R., Jerman-Blažič B. An economic modelling approach to information security risk management // International Journal of Information Management. 2008. № 28(5). С. 413–422.